Why use a VPN on Public Wi-Fi Networks

Posted At : July 30, 2018 10:37 AM | Posted By : Admin
Related Categories: Travel, Security, Wireless

Ithaca is a traveling community. The vast majority of our student population travels to and from Ithaca. Our business community and many individuals travel regularly for business. Virtually everyone who travels with a laptop, pad, or other mobile device usually ends up on some type of public Wi-Fi network. Getting to your data without exposing your private information to others takes effort. VPN technology is a good solution. The VPN discussed here is from Norton, but there are many other good ones as well.

If you've ever wondered if it's safe to use public Wi-Fi, you are not alone. In fact, according to the **Norton Cybersecurity Insights Report**, 6 in 10 consumers believe using public Wi-Fi is riskier than using a public restroom. And it is. Surfing the Web or transacting on an unsecured Wi-Fi network means you're placing your private information and anonymity at risk. That's why a virtual private network, better known as a VPN, is a must for anyone worried about online security and privacy.

What is a VPN?

A virtual private network gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your Internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections, guaranteed to provide greater privacy than even a secured Wi-Fi hotspot.

Why you need a VPN

Think about all the times you've been on the go, reading emails while in line at the coffee shop, or checking your bank account while waiting at the doctor's office. Unless you were logged into a private Wi-Fi network that required a password, any data transmitted during your online session was likely vulnerable to eavesdropping by strangers using the same network.

The encryption and anonymity that a VPN provides protects all of your online activities: sending emails, shopping online, or paying bills. VPNs also help keep your Web browsing anonymous.

Beyond security

VPNs essentially create a data tunnel between your local network and an exit node in another location, which could be thousands of miles away, making it seem as if you're in another place. This benefit makes VPNs valuable for people who live in countries that censor access to specific websites. It will also allow you to continue enjoying your favorite apps and websites from anywhere in the world, as if you were at home.

How to choose a VPN

The best way to stay secure when using public Wi-Fi is to use a VPN solution, like Norton WiFi Privacy, which is compatible with Android and iOS smartphones and tablets, as well as Windows PCs and Apple Macs. Here are some questions to ask when you're choosing a VPN provider.

1. **Do they respect your privacy?** The point of using a VPN is to protect your privacy, so it's crucial that your VPN provider respects your privacy, too. They should have a no-log policy, which means that they never track or log your online activities.
2. **Do they run the most current protocol?** OpenVPN provides stronger security than other

protocols, such as PPTP.

3. **Do they set data limits?** Depending on your Internet usage, bandwidth may be a large deciding factor for you. Make sure their services match your needs by checking to see if you'll get full, unmetered bandwidth without data limits. Remember, some packages may not cost you money, but you'll be subjected to frequent advertisements instead.

4. **Where are the servers located?** Decide which server locations are important to you. If you want to appear as if you're accessing the Web from a certain locale, make sure there's a server in that country.

5. **Will you be able to set up VPN access on multiple devices?** If you are like the average consumer, you use between three and five devices. Ideally, you'd be able to use the VPN on all of them at the same time.

6. **What happens if the VPN goes down?** Be sure that your provider implements a kill switch system in the event of failure. This means that your connection would automatically be locked down and would not default to an unsecured Internet connection if something goes wrong.

There are many points to consider when you're choosing a VPN, so do your homework to make sure you're getting the best fit for your needs. Regardless of which provider you choose, rest assured that any good VPN will provide far more security, privacy, and anonymity online than any public Wi-Fi hotspot ever could.